

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA

v.

KRASIMIR NIKOLOV

) Criminal No. 16-218
) [UNDER SEAL]
) (18 U.S.C. §§ 371, 1030(a)(2)(A),
) 1030(c)(2)(B)(i), 1344, and 2)
)

INDICTMENT

FILED

The grand jury charges:

OCT - 4 2016

INTRODUCTION

CLERK U.S. DISTRICT COURT
WEST. DIST. OF PENNSYLVANIA

At all times material to this indictment, unless otherwise alleged:

1) Malicious software (“malware”) is a software program designed to disrupt computer operations, gather sensitive information, gain access to private computer systems, or do other unauthorized action on a computer system. Common examples of malware include viruses, worms, Trojan horses, rootkits, keyloggers, spyware, and others.

2) “Internet Protocol address” or “IP address” is a unique numeric address used to identify computers on the Internet. The standard format for IP addressing consists of four numbers between 0 and 255 separated by dots, e.g., 149.101.10.40. Every computer connected to the Internet (or group of computers using the same account to access the Internet) must be assigned an IP address so that Internet traffic, sent from and directed to that computer, is directed properly from its source to its destination. Internet Service Providers (ISPs) assign IP addresses to their customers’ computers.

3) Keystroke logging is the action of recording (or logging) the keys struck on a keyboard. This action is usually done surreptitiously by a computer program (i.e., keylogger) to capture the keys typed on a computer without the typist’s knowledge. Malware

that uses keystroke logging often will provide the captured keystrokes to the individual who caused the malware to be installed or to a place designated by the individual. Through keystroke logging, individuals are able to obtain online banking credentials as soon as the user of the infected computer logs into their account. After obtaining this information, these individuals can access the victim's online bank account and execute unauthorized electronic funds transfers ("EFT"), such as Automated Clearing House ("ACH") payments or wire transfers,¹ to accounts that they control.

4) Web injects introduce (or inject) malicious computer code into a victim's web browser while the victim browses the Internet and "hijacks" the victim's Internet session. Different injects are used for different purposes. Some web injects are used to display false online banking pages into the victim's web browser to trick the victim into entering online banking information, which is then captured by the individual employing the web inject.

5) "Bot," which is short for "robot," is a computer that has been infected by malware and does tasks at the malware's direction.

6) A "botnet" is a network of bots. It is a collection of bots that can communicate with a computer controlling the botnet or with each other through some network architecture.

¹ Electronic funds transfers ("EFT") are the exchange and transfer of money through computer-based systems using the Internet. ACH payments allow the electronic transferring of funds from one bank account to another bank account within the ACH network without any paper money changing hands. The ACH network is a network of participating depository financial institutions across the United States, and the network provides for interbank clearing of electronic payments. Because ACH payments require the network to clear the transaction, the funds are not immediately available. Wire transfers also allow electronic transferring of funds from one bank account to another bank account without any paper money changing hands; however, unlike ACH payments, wire transferred funds are immediately available.

7) “Jabber” is an instant messaging platform that allows users to communicate in what are known as “chats” or “Jabber chats.” Jabber offers the user the ability to encrypt the communications.

8) “GozNym” is a multifunction malware package, which is specifically designed to automate the theft of confidential personal and financial information, such as online banking credentials, from infected computers through the use of keystroke logging and web injects.

9) Financial institutions in the United States first observed fraudulent activity related to GozNym in late 2015. GozNym is a hybrid of two previous malware families, Gozi and Nymaim.

10) GozNym malware is generally distributed through a process known as “phishing”, where spam emails are distributed to victims. The emails appear legitimate and are carefully crafted to entice the victim to click on a hyperlink or to open an attached file. In the event a user clicks on a hyperlink, the user is then usually redirected to an exploit kit, which is a web based software program that scans the victim’s computer and operating systems for vulnerabilities and upon discovering one, forces the download of a malicious file upon the victim. In the event the victim opens an attached file, he is then directly infected either by the GozNym malware, or by a loader program, which then downloads the GozNym payload without the victim’s consent or knowledge.

11) GozNym, like most modern malware families, is specifically crafted to defeat antivirus and other protective measures employed by victims.

12) A “mule” or “money mule” is a person who received stolen funds into their bank account, and then moved the money to other accounts, or withdrew the funds and transported the funds overseas as smuggled bulk cash.

13) First National Bank (FNB) was a financial institution insured by the Federal Deposit Insurance Corporation. FNB was headquartered in Pittsburgh, Pennsylvania, in the Western District of Pennsylvania. It offered online banking services, including providing the means to conduct electronic funds transfers, through computer servers located in the Western District of Pennsylvania.

14) PNC Bank (PNC) was a financial institution insured by the Federal Deposit Insurance Corporation. PNC was headquartered in Pittsburgh, Pennsylvania, in the Western District of Pennsylvania. It offered online banking services, including the means to conduct electronic funds transfers, through computer servers located in the Western District of Pennsylvania.

15) Protech Asphalt Maintenance, Inc. (Protech) was an asphalt and paving business located in New Castle, Pennsylvania, in the Western District of Pennsylvania.

16) Nord-Lock, Inc. (Nord-Lock) was a bolt manufacturing company located in Carnegie, Pennsylvania, in the Western District of Pennsylvania.

17) Foresight Sports, Inc. (Foresight) was a company that provided technology-based golf products and was located in San Diego, California.

18) California Furniture Collections, Inc. (d/b/a Artifacts International) was a furniture business located in Chula Vista, California.

19) The defendant, KRASIMIR NIKOLOV, was a citizen and resident of Bulgaria. NIKOLOV's primary role in the conspiracy charged in Count One was to utilize victims' stolen banking credentials acquired through GozNym malware infections of victims' computers to gain unauthorized access to victims' online bank accounts from which electronic funds transfers were issued or attempted to be issued.

COUNT ONE
(Conspiracy)

The grand jury further charges:

20) Paragraphs 1 through 19 above are hereby re-alleged and incorporated by reference herein, as if fully stated.

THE CONSPIRACY AND ITS OBJECTS

21) From in and around November 2015, the exact date being unknown to the grand jury, and continuing to on or about September 8, 2016, in the Western District of Pennsylvania and elsewhere, the defendant, KRASIMIR NIKOLOV, knowingly and willfully did conspire, combine, confederate, and agree with other persons known and unknown to the grand jury, to commit the following offenses against the United States:

(a) to intentionally access a computer, without authorization, and thereby obtain or attempt to obtain information in a financial record of a financial institution for the purpose of private financial gain, contrary to the provisions of Title 18, United States Code, Sections 1030(a)(2)(A) and 1030(c)(2)(B)(i), and 2;

(b) to devise, and intend to devise, a scheme and artifice to defraud businesses and individuals, and to obtain money from these businesses' and individuals' bank accounts and property, that is, confidential personal and financial information, by means of material false and fraudulent pretenses, representations, and promises, and for purpose of executing such scheme and artifice, to transmit, and cause to be transmitted, by means of wire communication in interstate and foreign commerce, certain writings, signs, signals, and pictures, contrary to the provisions of Title 18, United States Code, Sections 1343 and 2; and

(c) to knowingly execute, and attempt to execute, a scheme and artifice to defraud a financial institution and to obtain any of the moneys, funds, credits, assets, securities,

and other property owned by, and under the custody and control of, a financial institution by means of material false or fraudulent pretenses, representations, and promises, contrary to the provisions of Title 18, United States Code, Sections 1344 and 2.

22) The purpose of the conspiracy was to infect a user's computer with GozNym malware and capture the user's confidential personal and financial information, such as online banking credentials. The defendant, KRASIMIR NIKOLOV, and his co-conspirators used the captured information without authorization to falsely represent to banks that the defendant and co-conspirators were the victims or employees of the victims with authority to access the victims' bank accounts. The defendant, KRASIMIR NIKOLOV, and his co-conspirators subsequently caused or attempted to cause electronic funds transfers from the victims' bank accounts into the bank accounts of money mules.

MANNER AND MEANS OF THE CONSPIRACY

23) It was a part of the conspiracy that the defendant, KRASIMIR NIKOLOV, and co-conspirators known and unknown to the grand jury, sent phishing emails through the Internet that falsely represented themselves to be legitimate emails from legitimate companies, associations, and organizations.

24) It was further a part of the conspiracy that the defendant, KRASIMIR NIKOLOV, and co-conspirators known and unknown to the grand jury, created the phishing emails to fraudulently induce recipients to click on a hyperlink or attachment that falsely represented itself to be a legitimate link or attachment containing business or personal information, typically an attachment designed to appear as a legitimate business invoice, when in truth and fact, it installed malware on the email recipients' computers without the email recipients' consent or knowledge.

25) It was further a part of the conspiracy that the defendant, KRASIMIR NIKOLOV, and co-conspirators known and unknown to the grand jury, without authorization, installed and caused the installation of the GozNym malware on Internet-connected victim computers.

26) It was further a part of the conspiracy that the GozNym malware was designed to automate the theft of confidential personal and financial information, such as online banking credentials. The GozNym malware facilitated the theft of confidential personal and financial information by a number of methods. For example, the GozNym malware obtained such information through keystroke logging. Additionally, the GozNym malware allowed computer intruders to hijack a computer session and use web injects to present a fake online banking webpage to trick a user into entering personal and financial information.

27) It was further a part of the conspiracy that the defendant, KRASIMIR NIKOLOV, and co-conspirators known and unknown to the grand jury, used the GozNym malware on infected computers to capture the user's confidential personal and financial information, such as online banking credentials, by keystroke logging or by hijacking the computer session and presenting a web inject, i.e., fake online banking webpages.

28) It was further a part of the conspiracy that the defendant, KRASIMIR NIKOLOV, and co-conspirators known and unknown to the grand jury, used the captured confidential personal and financial information without authorization to falsely represent to banks that the defendant and co-conspirators were victims or employees of victims who had authorization to access the victims' bank accounts and to make electronic funds transfers from the victims' bank accounts.

29) It was further a part of the conspiracy that the defendant, KRASIMIR NIKOLOV, and co-conspirators known and unknown to the grand jury, targeted PayPal in

addition to banks, and used the captured confidential personal and financial information without authorization to falsely represent to PayPal that the defendant and co-conspirators were victims or employees of victims who had authorization to access the victims' PayPal accounts and to make electronic funds transfers from the victims' PayPal accounts.

30) It was further a part of the conspiracy that the defendant, KRASIMIR NIKOLOV, and co-conspirators known and unknown to the grand jury, used the captured banking credentials to cause and attempt to cause banks to make unauthorized wire transfers, ACH payments, or other electronic funds transfers from the victims' bank accounts, without the knowledge or consent of the account holders.

31) It was further a part of the conspiracy that, during the initial stages of developing GozNym, the defendant, KRASIMIR NIKOLOV, and co-conspirators known and unknown to the grand jury, created an administrative panel to assist them in conducting the scheme. The administrative panel was simply an interface hosted on a server that was configured to allow the co-conspirators to see the victims that had been infected with GozNym malware and their confidential banking information. The earliest of these administrative panels used the domain fokentoken.com hosted at IP address 204.155.30.87. Subsequent panels were hosted at IP address 204.155.31.133, and thereafter at IP address 204.155.30.8.

32) It was further a part of the conspiracy that the defendant, KRASIMIR NIKOLOV, and co-conspirators known and unknown to the grand jury, used money mules to receive the wire transfers, the ACH payments, or other electronic funds transfers from the victims' bank accounts.

Protech Asphalt Maintenance, Inc.

33) It was further a part of the conspiracy that, on or about February 18, 2016, the defendant, KRASIMIR NIKOLOV, and co-conspirators known and unknown to the grand jury, engaged in interstate and foreign wire communications over the Internet by sending to an

employee of Protech Asphalt Maintenance, Inc. (Protech), which was located in the Western District of Pennsylvania, a phishing email to fraudulently induce the employee to click on a graphic falsely represented to be a legitimate graphic.

34) It was further a part of the conspiracy that on or about February 18, 2016, the defendant, KRASIMIR NIKOLOV, and co-conspirators known and unknown to the grand jury, induced the Protech employee to click on the fraudulent graphic and, in so doing, caused the Protech employee to unwittingly install the GozNym malware on Protech Asphalt's computer.

35) It was further a part of the conspiracy that on or about February 24, 2016, the defendant, KRASIMIR NIKOLOV, and co-conspirators known and unknown to the grand jury, used the GozNym malware to fraudulently obtain the banking credentials of employees of Protech and attempted to cause the transfer of funds out of Protech's bank account maintained with First National Bank, which was located in the Western District of Pennsylvania.

36) It was further a part of the conspiracy that, on or about February 24, 2016, in the Western District of Pennsylvania, the defendant, KRASIMIR NIKOLOV, and co-conspirators known and unknown to the grand jury, fraudulently attempted to cause the following three electronic funds transfers in the amounts specified below totaling \$121,132.08, from Protech's account at First National Bank to the accounts specified below:

- a) \$74,287.80 to an account in the name of DCSH at Bank of America;
- b) \$39,856.88 to an account in the name of DCSH at Bank of America;
and
- c) \$6,987.40 to an account in the name of S.W. at Bank of America.

37) It was further a part of the conspiracy that, on or about April 11, 2016, the defendant, KRASIMIR NIKOLOV, sent to a co-conspirator the business name, "PROTECH

ASPHALT MAINTENANCE” as well as the business’ email account Protechasphalt@outlook.com.

38) It was further a part of the conspiracy that, on or about April 11, 2016, the defendant, KRASIMIR NIKOLOV, received from a co-conspirator information concerning four bank accounts, and the information included the following details:

- a) Type of Account: Personal
Holder Name: N.M.J.
Bank Name: Bank Midwest
Bank Address: Olathe, Kansas
ABA Routing Number: XXXXX6699
Wire Routing Number: XXXXX6699
Bank Account Number: XXXXXX7793
- b) Type of Account: Checking
Holder Name: J.P.
Bank Name: GoBank
Bank Address: Provo, Utah
Routing number ACH: XXXXX3162
Routing number WIRE: XXXXX3162
Bank Account Number: XXXXXXXXX2352
- c) Type of Account: Checking
Holder Name: K.H.
Bank Name: Wells Fargo
Bank Address: Brandon, Florida
Routing number ACH: XXXXX7513
Routing number WIRE: XXXXX7513
Bank Account Number: XXXXXX2862
- d) Type of Account: Checking
Holder Name: M.D.L.R
Bank Name: Chase
Bank Address: Palm Harbor, Florida
Routing number ACH: XXXXX4131
Routing number WIRE: XXXXX4131
Bank Account Number: XXXXXXXXXXXXX3770

39) It was further a part of the conspiracy that, on or about April 12, 2016, in the Western District of Pennsylvania, the defendant, KRASIMIR NIKOLOV, and co-

conspirators known and unknown to the grand jury, fraudulently attempted to cause the following four electronic funds transfers in the amounts specified below totaling \$122,000.00, from Protech's account at First National Bank to the accounts specified below:

- a) \$93,200.00 to Bank Account Number: XXXXXX7793 in the name of N.M.J. at Bank Midwest, Olathe, Kansas;
- b) \$9,600.00 to Bank Account Number: XXXXXXXX2352 in the name of J.P. at GoBank in Provo, Utah;
- c) \$9,600.00 to Bank Account Number: XXXXXX2862 in the name of K.H. at Wells Fargo Bank in Brandon, Florida; and
- d) \$9,600.00 to Bank Account Number: XXXXXX3770 in the name of M.D.L.R. at Chase Bank in Palm Harbor, Florida.

Nord-Lock, Inc.

40) It was further a part of the conspiracy that, on or about April 7, 2016, the defendant, KRASIMIR NIKOLOV, and co-conspirators known and unknown to the grand jury, engaged in interstate and foreign wire communications over the Internet by sending to an employee of Nord-Lock, Inc. (Nord-Lock), which was located in the Western District of Pennsylvania, a phishing email to fraudulently induce the employee to click on a graphic falsely represented to be a legitimate graphic.

41) It was further a part of the conspiracy that on or about April 7, 2016, the defendant, KRASIMIR NIKOLOV, and co-conspirators known and unknown to the grand jury, induced the Nord-Lock employee to click on the fraudulent graphic and, in so doing, caused the Nord-Lock employee to unwittingly install the GozNym malware.

42) It was further a part of the conspiracy that, on or about April 11, 2016, the defendant, KRASIMIR NIKOLOV, and co-conspirators known and unknown to the grand jury, fraudulently attempted to cause the electronic transfer of \$387,500.00 from Nord-Lock's account at PNC Bank to an account in the name of A.A. at D Commerce Bank, AD, in Sofia, Bulgaria.

Foresight Sports, Inc.

43) It was further a part of the conspiracy that, on or about May 23, 2016, the defendant, KRASIMIR NIKOLOV, and co-conspirators known and unknown to the grand jury, engaged in interstate and foreign wire communications over the Internet by sending to an employee at Foresight Sports, Inc., which was located in San Diego, California, a phishing email to fraudulently induce the employee to click on a graphic falsely represented to be a legitimate graphic.

44) It was further a part of the conspiracy that on or about May 23, 2016, the defendant, KRASIMIR NIKOLOV, and co-conspirators known and unknown to the grand jury, induced the Foresight Sports employee to click on the fraudulent graphic and, in so doing, caused the Foresight Sports employee to unwittingly install the GozNym malware on Foresight Sports' computer.

45) It was further a part of the conspiracy that on or about May 24, 2016, the defendant, KRASIMIR NIKOLOV, and co-conspirators known and unknown to the grand jury, used the GozNym malware to fraudulently obtain the banking credentials of employees of Foresight Sports and attempted to cause the transfer of funds out of Foresight Sports's bank account maintained with American Express.

46) It was further a part of the conspiracy that on or about May 24, 2016, the defendant, KRASIMIR NIKOLOV, received from a co-conspirator a message that contained the email account XXXXXXXXX@foresightsports.com along with an account passphrase XXXXXX14.

47) It was further a part of the conspiracy that on or about May 24 and 25, 2016, the defendant, KRASIMIR NIKOLOV, received from a co-conspirator a message that contained the bank account routing information for the following two bank accounts:

a) An account in the name C.H.E.L. at Fifth Third Bank in DeMotte, Indiana;

b) An account in the name K.T.E. at First Investment Bank in Bulgaria;

48) It was further a part of the conspiracy that, on or about May 26, 2016, and May 27, 2016, the defendant, KRASIMIR NIKOLOV, and co-conspirators known and unknown to the grand jury, fraudulently attempted to cause the following two electronic funds transfers in the amounts specified below totaling \$118,111.00, from Foresight Sports' account at American Express Foreign Exchange Service Payments to the accounts specified below:

a) \$67,000 to Bank Account Number: XXXXXX7613 in the name of C.H.E.L at Fifth Third Bank in DeMotte, Indiana on May 26, 2016; and

b) \$51,111 to Bank Account Number: XXXXXXXXXX5116 in the name of K.T.E. at First Investment Bank in Varna, Bulgaria on May 27, 2016.

California Furniture Collections, Inc.
(d/b/a Artifacts International)

49) It was further a part of the conspiracy that, on or about March 25, 2016, the defendant, KRASIMIR NIKOLOV, and co-conspirators known and unknown to the grand jury, engaged in interstate and foreign wire communications over the Internet by sending to an employee at California Furniture Collections, Inc., which was located in Chula Vista, California, a phishing email to fraudulently induce the employee to click on a graphic falsely represented to be a legitimate graphic.

50) It was further a part of the conspiracy that on or about March 25, 2016, the defendant, KRASIMIR NIKOLOV, and co-conspirators known and unknown to the grand jury, induced the California Furniture Collections employee to click on the fraudulent graphic and, in so doing, caused the employee to unwittingly install the GozNym malware on California Furniture Collections' computer.

51) It was further a part of the conspiracy that on or about March 25, 2016, the defendant, KRASIMIR NIKOLOV, and co-conspirators known and unknown to the grand jury, used the GozNym malware to fraudulently obtain the banking credentials of employees of California Furniture Collections and attempted to cause the transfer of funds out of California Furniture Collections's bank account maintained with CommerceWest Bank.

52) It was further a part of the conspiracy that on or about March 25, 2016, the defendant, KRASIMIR NIKOLOV, sent to a co-conspirator a message that contained the email address XXXXXX@artifactsinternational.com along with an account passcode "XXXXXX1959!."

53) It was further a part of the conspiracy that on or about March 25, 2016, the defendant, KRASIMIR NIKOLOV, sent to a co-conspirator a message that contained the following information: "\$70,000.00 03/25/2016 California Furniture Collectio T.L.V.T. Ltd." XXXXXXXXXXXXXXXXXXXX2001500.

54) It was further a part of the conspiracy that, on or about March 25, 2016, the defendant, KRASIMIR NIKOLOV, and co-conspirators known and unknown to the grand jury, fraudulently attempted to cause ten electronic funds transfers in the amounts specified below totaling \$737,550.00, from California Furniture Collections' account at CommerceWest Bank to an account in the name of T.L.V.T. Ltd. at VTB Bank in Tbilisi, Georgia:

- a) Six attempted transfers each in the amount of \$70,000; and
- b) Four attempted transfers each in the amount of \$79,387.50.

OVERT ACTS

55) In furtherance of the conspiracy, and to effect the objects of the conspiracy, the defendant, KRASIMIR NIKOLOV, and co-conspirators both known and unknown to the grand jury, did commit and cause to be committed, the following overt acts, among others, in the Western District of Pennsylvania and elsewhere:

(a) On or about November 23, 2015, the defendant, KRASIMIR NIKOLOV, received a message from a co-conspirator containing the following URL:

<http://fokentoken.com/concert5/index.php?r=admin/checker&hash=0ac8a51a2b27a3e2f9d61166c1bf7f02>, and a password “qwerty123”

(b) On or about December 7, 2015, the defendant, KRASIMIR NIKOLOV, received a message from a co-conspirator that explained how to login to the fokentoken administrative panel.

(c) On or about January 15, 2016, the defendant, KRASIMIR NIKOLOV, received a message from a co-conspirator that contained the IP address 204.155.31.133 for the subsequent administrative panel.

(d) On or about January 25, 2016, the defendant, KRASIMIR NIKOLOV, received a message from a co-conspirator that contained information for a fraudulent invoice, consistent with the invoices used in the GozNym phishing emails that were designed to appear legitimate to entice the recipient to click on it.

(e) On or about February 18, 2016, the defendant, KRASIMIR NIKOLOV, and co-conspirators sent to an employee at Protech Asphalt Maintenance, Inc., located within the Western District of Pennsylvania, a phishing email, in order to cause the GozNym malware to be installed on an Internet-connected computer used by Protech, without the Protech employee’s consent or knowledge.

(f) On or about February 18, 2016, the defendant, KRASIMIR NIKOLOV, and co-conspirators caused the GozNym malware to be installed, without authorization, on Protech’s Internet-connected computer located in the Western District of Pennsylvania.

(g) On or about April 11, 2016, the defendant, KRASIMIR NIKOLOV, sent to a co-conspirator the business name, "PROTECH ASPHALT MAINTENANCE" as well as the business' email account Protechasphalt@outlook.com.

(h) On or about April 11, 2016, the defendant, KRASIMIR NIKOLOV, received from a co-conspirator information concerning four bank accounts, and the information included the following details:

- i. Type of Account: Personal
Holder Name: N.M.J.
Bank Name: Bank Midwest
Bank Address: Olathe, Kansas
ABA Routing Number: XXXXX6699
Wire Routing Number: XXXXX6699
Bank Account Number: XXXXXX7793
- ii. Type of Account: Checking
Holder Name: J.P.
Bank Name: GoBank
Bank Address: Provo, Utah
Routing number ACH: XXXXX3162
Routing number WIRE: XXXXX3162
Bank Account Number: XXXXXXXXX2352
- iii. Type of Account: Checking;
Holder Name: K.H.;
Bank Name: Wells Fargo;
Bank Address: Brandon, Florida;
Routing number ACH: XXXXX7513;
Routing number WIRE: XXXXX7513;
Bank Account Number: XXXXXX2862.
- iv. Type of Account: Checking
Holder Name: M.D.L.R
Bank Name: Chase
Bank Address: Palm Harbor, Florida
Routing number ACH: XXXXX4131
Routing number WIRE: XXXXX4131
Bank Account Number: XXXXXXXXXXXXX3770

(i) On or about April 12, 2016, the defendant, KRASIMIR NIKOLOV, and co-conspirators fraudulently attempted to cause four electronic funds transfers in the amounts specified below totaling \$122,000.00, from Protech's account at First National Bank, in the Western District of Pennsylvania, to the accounts specified below:

- i. \$93,200.00 to Bank Account Number: XXXXXX7793 in the name of N.M.J. at Bank Midwest, Olathe, Kansas;
- ii. \$9,600.00 to Bank Account Number: XXXXXXXX2352 in the name of J.P. at GoBank in Provo, Utah;
- iii. \$9,600.00 to Bank Account Number: XXXXXX2862 in the name of K.H. at Wells Fargo Bank in Brandon, Florida; and
- iv. \$9,600.00 to Bank Account Number: XXXXXX3770 in the name of M.D.L.R. at Chase Bank in Palm Harbor, Florida.

(j) On or about May 3, 2016, the defendant, KRASIMIR NIKOLOV, received a message from a co-conspirator that contained the IP address 204.155.30.8 for the subsequent administrative panel.

(k) On or about May 24, 2016, the defendant, KRASIMIR NIKOLOV, received from a co-conspirator a message that contained the email account XXXXXXXX@foresightsports.com along with an account passphrase XXXXXX14.

(l) On or about May 24 and 25, 2016, the defendant, KRASIMIR NIKOLOV, received from a co-conspirator a message that contained the bank account routing information for the following two bank accounts:

- i. An account in the name C.H.E.L. at Fifth Third Bank in DeMotte, Indiana;
- ii. An account in the name K.T.E. at First Investment Bank in Bulgaria;

(m) On or about May 26, 2016 and May 27, 2016, the defendant, KRASIMIR NIKOLOV, and co-conspirators fraudulently attempted to cause the following two electronic funds transfers in the amounts specified below totaling \$118,111.00, from Foresight Sports' account at American Express Foreign Exchange Service Payments to the accounts specified below:

- i. \$67,000 to an account in the name of C.H.E.L. at Fifth Third Bank in DeMotte, Indiana on May 26, 2016; and
- ii. \$51,111 to an account in the name of K.T.E. at First Investment Bank in Varna, Bulgaria on May 27, 2016.

(n) On or about March 25, 2016, the defendant, KRASIMIR NIKOLOV, sent to a co-conspirator a message that contained the email address "XXXXXX@artifactsinternational.com" along with an account passcode "XXXXXX1959!."

(o) On or about March 25, 2016, the defendant, KRASIMIR NIKOLOV, sent to a co-conspirator a message that contained the following information: "\$70,000.00 03/25/2016 California Furniture Collectio T.L.V.T. Ltd." XXXXXXXXXXXXXXXXXXXX2001500.

(p) On or about March 25, 2016, the defendant, KRASIMIR NIKOLOV, and co-conspirators fraudulently attempted to cause ten electronic funds transfers in the amounts specified below totaling \$737,550.00, from California Furniture Collections' account at CommerceWest Bank to an account in the name of T.L.V.T. Ltd. at VTB Bank in Tbilisi, Georgia:

- i. Six attempted transfers each in the amount of \$70,000; and
- ii. Four attempted transfers each in the amount of \$79,387.50.

(q) On or about September 8, 2016, the Defendant logged into the administrative panel hosted at IP address 204.155.30.8.

All in violation of Title 18, United States Code, Section 371.

COUNT TWO

(Unauthorized Access of a Computer to Obtain Financial Information)

The grand jury further charges:

56) Paragraphs 1 through 19 and 23 through 55 above are hereby re-alleged and incorporated by reference herein, as if fully stated.

57) On or about the April 12, 2016, in the Western District of Pennsylvania and elsewhere, the defendant, KRASIMIR NIKOLOV, intentionally accessed a computer, without authorization, and thereby obtained information contained in a financial record of a financial institution, that is the defendant, KRASIMIR NIKOLOV, accessed, and caused to be accessed, information from a financial record of First National Bank pertaining to the bank account of Protech Asphalt Maintenance, Inc., said offense was committed for the purpose of private financial gain.

In violation of Title 18, United States Code, Sections 1030(a)(2)(A), 1030(c)(2)(B)(i), and 2.

COUNTS THREE THROUGH SIX
(Bank Fraud)

The grand jury further charges:

58) Paragraphs 1 through 19, and 23 through 55 above are hereby re-alleged and incorporated by reference herein, as if fully stated.

59) On or about the dates set forth below, in the Western District of Pennsylvania and elsewhere, the defendant, KRASIMIR NIKOLOV, having devised and intended to devise a scheme and artifice to defraud First National Bank to obtain monies and funds owned by and under the custody and control of First National Bank by means of material false and fraudulent pretenses, representations and promises, well knowing at the time that the pretenses, representations and promises would be and were false and fraudulent when made, did knowingly execute, and attempt to execute, the foregoing scheme and artifice, by causing, and attempting to cause, the transfer of funds, with each such transfer and attempted transfer being a separate count of this indictment as described below:

Count	On or About Date	Description
3	April 12, 2016	The attempted electronic funds transfer of \$93,200.00 from Protech Asphalt's account at First National Bank to bank account number XXXXXX7793 in the name of N.M.J. at Bank Midwest, Olathe, Kansas.
4	April 12, 2016	The attempted electronic funds transfer of \$9,600.00 from Protech Asphalt's account at First National Bank to bank account number XXXXXXXX2352 in the name of J.P. at GoBank in Provo, Utah.
5	April 12, 2016	The attempted electronic funds transfer of \$9,600.00 from Protech Asphalt's account at First National Bank to bank account number XXXXXX2862 in the name of K.H. at Wells Fargo Bank in Brandon, Florida.
6	April 12, 2016	The attempted electronic funds transfer of \$9,600.00 from Protech Asphalt's account at First National Bank to bank account number XXXXXX3770 in the name of M.D.L.R. at Chase Bank in Palm Harbor, Florida.

In violation of Title 18, United States Code, Sections 1344 and 2.

FORFEITURE ALLEGATION I

60) The allegations contained in Count One and Count Two of this Indictment are hereby re-alleged and incorporated by reference for the purpose of alleging forfeitures pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i).

61) Upon conviction of the offenses in violation of Title 18, United States Code, Sections 371, and 1030(a)(2)(A) and 1030(c)(2)(B)(i), set forth in Count One and Count Two of this Indictment, the defendant, KRASIMIR NIKOLOV, shall forfeit to the United States of America:

a. pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i), any property, real or personal, constituting, or derived from, proceeds obtained directly or indirectly as a result of such offense, such property includes but is not limited to a money judgment for a sum of money equal to the proceeds obtained as a result of the offense; and

b. pursuant to Title 18, United States Code, Section 1030(i), any personal property that was used or intended to be used to commit or to facilitate the commission of such offense.

62) If through any acts or omission by the defendant, KRASIMIR NIKOLOV, any or all of the property described in paragraphs 60 and 61 above (hereinafter the "Subject Properties"):

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third party;

c. has been placed beyond the jurisdiction of the court;

d. has been substantially diminished in value; or

e. has been commingled with other property which cannot be divided without difficulty,

the United States of America shall be entitled to forfeiture of substitute property pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Sections 982(b) and 1030(i).

All pursuant to Title 18, United States Code, Sections 982(a)(2)(B), 982(b) and 1030(i), Title 21, United States Code, Section 853, and Title 28 U.S.C. § 2461(c).

FORFEITURE ALLEGATION II

63) The allegations contained in Counts Three through Six of this Indictment are hereby re-alleged and incorporated by reference for the purpose of alleging forfeitures pursuant to Title 18, United States Code, Section 981(a)(1)(C) and 28 United States Code, Section 2461(c).

64) Upon conviction of the offenses in violation of Title 18, United States Code, Sections 1344 and 2 set forth in Counts Three through Six of this Indictment, the defendant, KRASIMIR NIKOLOV, shall forfeit to the United States of America, pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c), any property, real or personal, which constitutes, and is derived from, proceeds traceable, directly and indirectly, to such violations. The property to be forfeited includes, but is not limited to, a money judgment for a sum of money equal to the proceeds obtained as a result of the offenses.

65) If through any acts or omission by the defendant, KRASIMIR NIKOLOV, any or all of the property described in paragraphs 63 and 64 above (hereinafter the "Subject Properties"):


- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third party;
- c. has been placed beyond the jurisdiction of the court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property which cannot be divided without difficulty,

the United States of America shall be entitled to forfeiture of substitute property pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 28, United States Code, Section 2461(c).

All pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c).

A True Bill,


FOREPERSON


DAVID J. HICKTON
United States Attorney
PA ID No. 34524